STATE OF ALABAMA

Information Technology Standard

Standard 680-03S1_Rev B: Encryption

1. INTRODUCTION:

Encryption is a technique used to help protect the confidentiality of stored or transmitted information. As required in this and other State standards, encryption must be utilized to protect sensitive and confidential information. Security Management Plans must address the required level of information protection taking into account the method of encryption used, key management strategies, and the length of cryptographic keys employed.

2. OBJECTIVE:

Provide the minimum requirements for the selection, application, and management of encryption technology.

3. SCOPE:

These requirements apply to sensitive or confidential systems; to sensitive or confidential data accessed, stored, or transmitted on State and public networks; and to sensitive or confidential data recorded or stored on portable devices.

4. REQUIREMENTS:

4.1 ENCRYPTION UTILIZATION

Use encryption to protect sensitive and confidential systems and information as specified in this and other applicable standards and when other controls do not provide adequate protection.

Users accessing sensitive and confidential systems or information from outside State or agency networks must encrypt the session.

Laptops, notebooks, tablet PCs, and similar devices shall utilize full-disk encryption (FDE).

Encrypt sensitive and confidential data on portable data storage devices (PDA, flash drive, CD, DVD, or any other external storage device) whenever technically possible.

4.2 ENCRYPTION METHODS

The use of proprietary encryption algorithms, an algorithm that has not been made public and/or has not withstood public scrutiny (regardless of whether the developer of the algorithm is a vendor, an individual, or the government) is not allowed for any purpose.

Encryption products used shall be listed on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation List (http://csrc.nist.gov/groups/STM/cmvp/validation.html) and be validated to the current Federal Information Processing Standard (FIPS).

4.2.1 Acceptable Methods

Encryption methods that utilize either the Triple Data Encryption Standard (Triple DES) or the Advanced Encryption Standard (AES) are acceptable. Encryption methods shown below can also be used to protect sensitive and confidential information:

- Virtual Private Network (VPN) – allows information to be sent securely between two end stations or networks over an un-trusted communications medium; use of VPN technology is the preferred method for securing sensitive and confidential communications.
- IPSEC – is suitable for all types of Internet Protocol (IP) traffic, and may be used to secure Internet and other IP communications within State and agency networks and to connect to authorized external customers.
- Secure Sockets Layer (SSL) – may be deployed to provide secured access to sensitive and confidential information on Web servers.
- Secure Shell (SSH) – may be utilized for the remote administration of sensitive systems.
- Approved Hash Algorithms: SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. (SHA-1 may not be suitable for digital signature application requiring greater than 80 bits security unless using the randomized hashing technique described in NIST Special Publication 800-106). Other hashing methods, some in wide-spread use such as MD5, are not recommended.

Other methods of encryption require explicit approval of the State IT Security Council before being used to protect State data or systems.

4.2.2 Unacceptable Methods

Unacceptable methods of encryption include:

- Data Encryption Standard (DES)
- Wired Equivalent Privacy (WEP)

4.3 KEY LENGTH

Symmetric cryptosystems (such as AES) require a minimum 128 bit key length.

Asymmetric cryptosystems (such as RSA) require key lengths equivalent to a 128 bit or longer symmetric key. Example: A 3072-bit RSA key is equivalent to a 128-bit symmetric key.

The State IT Security Council shall conduct annual review of key length and other encryption requirements when scheduled to conduct the annual review of this standard.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 680-03: Encryption
http://isd.alabama.gov/policy/Policy_680-03_Encryption.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Information Technology Standard 680-01S1: Information Protection
http://isd.alabama.gov/policy/Standard_680-01S1_Information_Protection.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	5/23/2006	
Rev A	11/2/2007	Revised requirement for laptops
Rev B	8/5/2008	Section 4.2: restated Cryptographic Module Validation as a requirement; added hashing methods